UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,932	01/12/2001	William T. Daniell	10004557-1	2759

7590 03/09/2005

HEWLETT PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/759,932	DANIELL ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 have been examined and are pending.

Claims 1, 8-9 are amended.

Claims 11-24 are newly added.

Response to Amendment

2. Applicant's arguments filed 11/8/2004 regarding the rejection of the claims 1-10 under 35 U.S.C. 102 and 103 have been fully considered but they are not persuasive.

As per Applicant arguments relating to the rejection of claims 1, 5 and 8, Applicant argues that the Pereira fails to disclose "said security application configured to store, in said memory, data indicative of said security settings, said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison" and that "there is nothing in Pereira to indicate that such a "security setting" change is detected based on a comparison between the alleged "data" of the registry file and the alleged "security setting.", pages 10-11 of the REMARKS.

The Examiner responds that Pereira teaches (col. 7, lines 49-67) an exemplary display is shown (FIG. 2) where the Primary User may view a list of authorized users in window 50. To add a user, the primary user activates the new user function which causes the display of FIG. 3 to appear so the primary user can enter the user's name and resource parameters. In response to the closing of the manage users function, the access control program generates a file of authorized

user identifiers and, as each user supplies a password, the file is updated with each user's corresponding password. This file is used by the access control program to limit access to the system to authorized users only (i.e. security application configured to store, in said memory, data indicative of said security settings). Pereira teaches (col. 10, line) the access control program modifies the registry file used to define system resources to prevent default user from gaining control of the system resources and that if the user enters corresponding password, however, the file identified by the user's identifier are used to define the resources in the registry file. Then, the system only displays the ones which the primary user identified (i.e. security application configured to perform comparisons between the data and the security setting) and that if the user (col. 10, line 64, col. 11, line 10) is able to find and modify one program component to access unauthorized resources, the other two programs components detect the change. In response to a detected change, the program component resets the system of that all three program components are reloaded from the hard disk to memory to overwrite the changed program component.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. **Claims 1, 3-5, 7-8, 10-23** are rejected under 35 U.S.C. 102(b) as being anticipated by prior art of record, Pereira (USP 5,809,230).

As per claim 1, Pereira teaches memory (col.7, lines 49-64, column 10, line 11,), and a security application configured display a list of security rules to a user and to enable ones of said security rules based on user inputs (see figure 4), said security application configured to lock down resources of said computer system by modifying security settings of said computer system based on which of said security rules are enabled when an activation request is received by said computer system (col. 10, lines 10- 33, column 3, line 64-column 4, line 3), said security application configured to store, in said memory, data indicative of said security settings (column 10, lines 10-13), said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison (column 10, lines 64-column 11, line 6).

As per claims 5 and 8, Pereira teaches receiving a request for activating a security profile (column 7, lines 49-53), modifying security settings of said computer system based on said request (see figure 4), store said data in response to said activation request (column 4, lines 33-35), automatically determine when on of said security settings has changed from a first value to another by periodically comparing said data to said security settings (column 10, lines 64-column 11, line 3), automatically changing one security setting to said first value in response to a determination that one security setting has changed (column 11, lines 3-6).

As per claims 3, 7, and 10, Pereira teaches said security application is further configured to store said data in response to said activation request (column 9, lines 2933).

As per claim 4, Pereira teaches said security application is further configured to periodically compare each of said security settings to said data (column 11, lines 2-3).

As per claim 11, Pereira teaches wherein said security application is configured to change said one security setting in response to said one comparison without changing another of said security settings in response to said one comparison [col. 4, lines 14-31].

As per claims 12, 18-19, Pereira teaches that an operating system configured to analyze said one security setting to determine whether access to a resource of said computer system is restricted [col. 6, lines 50-67, see also col. 7, lines 27-34].

As per claim 13 and 14, Pereira teaches wherein said one security setting is associated with one of said security rules [col. 9, line 44, col. 10, line9], and wherein said operating system is configured to enforce said one security rule based on said one security setting [col. 10, lines 10-33, i.e. Windows 95 uses access file to display program icons and program groups] and that said security application is not configured to enforce said one security rule.

As per claim 15, Pereira teaches wherein said security settings are within a machine state analyzed by said operating system for selectively enforcing said security rules [col. 12, lines 26-32].

As per claim 16, Pereira teaches wherein said data is separate [col. 6, lines 53-67, i.e. the security program uses the DPMI regardless of weather DOS or windows is operating] from said machine state and is stored in said memory by said security application in response to said activation request.

As per claim 17, Pereira teaches wherein said one security setting is a flag associated with said resource [col. 12, lines 28-32, i.e. interrupts (i.e. flag associated with the resources) to

access the hard disk are intercepted by one of the program components which use the modified MBR program and restored partition table and boot record to control access to the hard disk].

As per claim 20, Pereira teaches a computer system, comprising: memory [col. 10, line 11];

an operating system configured to analyze a machine state to control operation of said computer system, said machine state including a security setting associated with a resource of said computer system and indicating whether access to said resource is restricted, wherein said operating system is configured to analyze said security setting to control access to said resource [col. 4, lines 10-31, Pereira teaches On PCs implementing a Windows program type interface, the list of the computer resources are preferably kept in files which are used to modify Group and INI files through the Dynamic Data Exchange (DDE). The modified system files are used to display group and program icons which may be activated by a user to launch a program. Once the system files have been modified, the access control program prevents a user from restoring the deleted group displays and programs to the system files. Thus, the user cannot restore deleted group displays and programs even if the user knows the file names for deleted resources. To restore the system files for the next user, the method of the present invention encrypts and stores an unabridged version of the system files which contain all of the groups and programs which are available on the system to a user having no limitations. At the system start-up for each user, the method retrieves and decrypts the unabridged version and deletes those programs and groups not contained in the corresponding list for the user. In this way, the system may be configured to only display the authorized resources for each user without losing a reference to all programs and groups possible on the system.];and

a security application configured to modify said security setting (i.e. the access control program modifies the registry file used to define system resources to prevent default user from gaining control of the system resources) based on a user input [col. 7, lines 49-53, see fig. 4) and to store, in said memory, data indicative of a state of said security setting (i.e. , at the system start-up for each user, the method retrieves and decrypts the unabridged version and deletes those programs and groups not contained in the corresponding list for the user] application, said security application configured to perform a comparison between said data and said security setting to detect an unauthorized change of said security setting [col. 10, line 64, col. 11,line 10] said security application further configured to automatically change said security setting based on said data in response to a detection of an unauthorized change of said security setting [i.e. to restore the system files for the next user, the method encrypts and stores an unabridged version of the system files which contain all of the groups and programs which are available on the system to a user having no limitations].

As per claim 21, Pereira teaches wherein said security application is configured to set said security setting based on said user input in response to a user activation request [col. 7, lines 49-53].

As per claim 22, Pereira teaches wherein said security application is configured to store said data in said memory in response to said user activation request Fig.3, i.e. the primary user activates the new user function which causes a display (fig.3) to appear so the primary user can enter the user's name and resource parameters].

As per claim 23, Pereira teaches wherein said security setting is a flag stored within a register [col. 12, lines 28-32, i.e. interrupts (i.e. flag associated with the resources) to access the

hard disk are intercepted by one of the program components which use the modified MBR program and restored partition table and boot record to control access to the hard disk].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 2, 6, 9 and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Pereira in view of prior art of record, Proctor (USP 6,530,024).

As per claims 2, 6, and 9 and 24, Pereira is silent in disclosing that a message is automatically sent in response to a security setting being changed. Proctor's security system automatically sends a message by alerting the administrator whenever network policies have been updated (column 21, line 64--column 3, line 3).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Proctor within the system of Pereira because it would immediately bring potentially harmful network event to the attention of the administrator so that lie/she can respond accordingly. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Action is Final

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. A.

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

Gilberto Barron Jr.

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100